UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,730	03/31/2004	Bruce Edward LaVigne	200314975-1	5129

22879 7590 02/18/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
ALMEIDA, DEVIN E	
ART UNIT	**PAPER NUMBER**
2432	

NOTIFICATION DATE	DELIVERY MODE
02/18/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/813,730
Filing Date: March 31, 2004
Appellant(s): LAVIGNE ET AL.

For Appellant
Ashok Mannava
REG 45301

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11/03/2009 appealing from the Office action mailed 8/03/2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

NEW GROUND(S) OF REJECTION

Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Regan (U.S. 2004/0213232) in view of Inada et al (U.S. Patent # 6,775,769) in view of Amara et al (U.S. Patent # 6,839,338) in further view of Kojima et al (5,280,476).

Amara et al (U.S. Patent # 6,839,338) was inadvertently left out of the heading. Claim 5 depends from claim 1 in which Amara et al (U.S. Patent # 6,839,338) was part of the rejection.

Claim 13, rejected under 35 U.S.C. 103(a) as being unpatentable over Regan (U.S. 2004/0213232) in view of Inada et al (U.S. Patent # 6,775,769) in view of Amara et al (U.S. Patent # 6,839,338) in view of Engwer (U.S. Patent 6,947,483).

Amara et al (U.S. Patent # 6,839,338) was inadvertently left out of the heading. Claim 13 depends from claim 1 in which Amara et al (U.S. Patent # 6,839,338) was part of the rejection.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

20040213232	Regan	10-2004
6,775,769	Inada et al	8-2004
6,839,338	Amara et al	1/2005
5,280,476	Kojima et al	1-1994

6,700,867	Classon et al	3-2004
6,947,483	Engwer	9-2005

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 4, 7-11, 14, and 16-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Regan (2004/0213232) in view of Inada et al (U.S. Patent # 6,775,769) in further view of Amara et al (U.S. Patent # 6,839,338).

Regan teaches with respect to claim 1, a method for secure remote mirroring of network traffic, the method comprising: receiving a data packet to be remotely mirrored by an entry device (see Regan abstract i.e. data packets, segments, frames, or other forms of encapsulation may be mirrored off of a core network (e.g., IP, TCP) to one or more mirroring destinations without using a parallel network)) pre-configured with a mirroring destination address to which to mirror the data packet (see Regan abstract and paragraph 0022 i.e. a forwarding engine 202 may be implemented as one or more modules used for both mirroring and forwarding packets from a router to a primary destination (i.e., a destination to which the packet is addressed) and a mirror destination (i.e., the place to which you want the mirror packets to be sent));

forwarding the data packet in unencrypted form towards an original destination address indicated in the data packet and a copy to a mirror destination (see Regan abstract and paragraph 0022-0026); and

forwarding the encapsulated packet to an exit device associated with the mirroring destination address (see paragraph 0023 i.e. a forwarding engine 202 may be implemented as one or more modules used for both mirroring and forwarding packets from a router to a primary destination (i.e., a destination to which the packet is addressed) and a mirror destination (i.e., the place to which you want the mirror packets to be sent)).

Regan does not teach encrypting a copy the data packet to form an encrypted packet; incrementing an identifier for indicating a position of the data packet within an order of packets received by an exit device; generating and adding a first header and a second header to the encrypted data packet to encapsulate the encrypted data packet, wherein the first header includes an Internet Protocol destination address corresponding to the destination address and said identifier, the second header includes a media access control (MAC) destination address, and the encapsulated encrypted packet comprises an IP-encapsulated encrypted packet including the IP destination address.

Regan teaches that the mirrored packet are encapsulated and sent via a transport tunnel (see paragraph 0025) but does not go into the way the packets are encapsulated.

Inada teaches encrypting a copy the data packet to form an encrypted packet (see column 11 lines 43-52 i.e. encrypts the whole received plaintext pack); generating and adding a first header and a second header to the encrypted data packet to encapsulate the encrypted data packet, wherein the first header includes an Internet Protocol destination address corresponding to the destination address and said

identifier (see column 11 lines 43-52 i.e. set new IP header), the second header includes a media access control (MAC) destination address (see column 11 lines 43-52 i.e. then, the ciphertext MAC address resolution block 28 sets the MAC address of the MAC header based on the IP address of the IP header newly set), and the encapsulated encrypted packet comprises an IP-encapsulated encrypted packet including the IP destination address (see column 11 lines 43-52);

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used the encapsulation as taught by Inada to encrypt and encapsulate the data packet to further increase the security of the data packet by not allowing other devices to intercept the IP packet and read its data portion (see Inada column 13 lines 39-57). Therefore one would have been motivated to have used the encapsulation as taught by Inada.

Amara teaches incrementing an identifier for indicating a position of the data packet within an order of packets received by an exit device (see Figure 4 element 210 sequence number and column 8 lines 5-24). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a sequence number is used to keep track of each data packet. Therefore one would have been motivated to have a sequence number for each packet.

With respect to claim 4 determining the MAC destination address associated with the destination IP address; generating and adding as the second header a MAC header including the MAC destination address to the IP-encapsulated packet to form a MAC data frame, wherein the MAC header includes the MAC destination address in a

destination field; and transmitting the MAC data frame to communicate the IP-encapsulated packet across a layer 2 domain (see column 11 lines 43-52 i.e. then, the ciphertext MAC address resolution block 28 sets the MAC address of the MAC header based on the IP address of the IP header newly set).

With respect to claim 7, further comprising: receiving the encapsulated encrypted packet by the exit device (see Amara column 8 line 66 – column 9 line 15 i.e. the destination device endpoint); removing the header to de-encapsulate the encrypted packet; and decrypting the encrypted packet to re-generate the data packet (see Amara column 8 line 66 – column 9 line 15 i.e. the destination device endpoint decrypts the original IP packet and forwards that packet to the destination device); and using said identifier to determine the position of the data packet within the order of packets received by the exit device (see Amara Figure 4 element 210 sequence number and column 8 lines 5-24).

With respect to claim 8, wherein the encrypting and decrypting is performed under a public-private key encryption scheme (see Amara column 10 lines 6-60).

With respect to claim 9, wherein the encrypting is performed using a public key of a destination device, and wherein the decrypting is performed using a corresponding private key of the destination device (see Amara column 10 lines 6-60).

With respect to claim 10, configuring the entry device in a best effort mirroring mode to reduce head-of-line blocking (see Amara abstract and column 8 line 66 – column 9 line 15).

With respect to claim 11, configuring the entry device in a lossless mirroring mode to assure completeness of mirrored traffic (see Amara abstract and column 8 line 66 – column 9 line 15).

With respect to claim 14, a networking device comprising:

a plurality of ports for receiving and transmitting packets therefrom, wherein the packets are transmitted based on original destination address indicated therein (see Regan abstract and paragraph 0022 i.e. a forwarding engine 202 may be implemented as one or more modules used for both mirroring and forwarding packets from a router to a primary destination (i.e., a destination to which the packet is addressed) and a mirror destination (i.e., the place to which you want the mirror packets to be sent));

a secure remote mirroring engine configured to detect packets from a specified mirror source, and to forward the encapsulated encrypted packets to a pre-configured destination address corresponding to the IP destination address by way of at least one of the ports (see Regan abstract and paragraph 0022 i.e. a forwarding engine 202 may be implemented as one or more modules used for both mirroring and forwarding packets from a router to a primary destination (i.e., a destination to which the packet is addressed) and a mirror destination (i.e., the place to which you want the mirror packets to be sent)).

Regan does not teach to use an incrementing identifier to indicating an order of the detected packets, to encrypt the detected packets, to encapsulate each of the encrypted packets by adding to the encrypted packet a first header which includes said identifier and an internet Protocol destination address and by also adding a second

header which includes a media access control destination address, and an encryption module configured to be utilized by the remote mirroring engine during encryption of the detected packets.

Regan teaches that the mirrored packet are encapsulated and sent via a transport tunnel (see paragraph 0025) but does not go into the way the packets are encapsulated.

Inada teaches to encrypt the detected packets (see column 11 lines 43-52 i.e. encrypts the whole received plaintext pack), to encapsulate each of the encrypted packets by adding to the encrypted packet a first header which includes said identifier and an internet Protocol destination address (see column 11 lines 43-52 i.e. set new IP header) and by also adding a second header which includes a media access control destination address (see column 11 lines 43-52 i.e. then, the ciphertext MAC address resolution block 28 sets the MAC address of the MAC header based on the IP address of the IP header newly set).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used the encapsulation as taught by Inada to encrypt and encapsulate the data packet to further increase the security of the data packet by not allowing other devices to intercept the IP packet and read its data portion (see Inada column 13 lines 39-57). Therefore one would have been motivated to have used the encapsulation as taught by Inada.

Amara teaches incrementing an identifier for indicating a position of the data packet within an order of packets received by an exit device (see Figure 4 element 210

sequence number and column 8 lines 5-24). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a sequence number is used to keep track of each data packet. Therefore one would have been motivated to have a sequence number for each packet.

With respect to claim 16, The networking device of claim 15, wherein the remote mirroring engine encrypts the copies of the detected packets using a public key of a public-private key pair (see Amara column 10 lines 6-60).

With respect to claim 17, a system for secure remote mirroring of network traffic, the system comprising: a mirror entry device including a secure mirroring engine configured to detect packets from a specified mirror source, and to forward the encapsulated encrypted packets to a pre-configured destination by way of at least one of the ports, wherein the pre-configured destination is distinct from original destination indicated in the detected packets, and wherein the detected packets are forwarding in unencrypted form towards an original destination address indicated in the data packet (see Regan abstract and paragraph 0022 i.e. a forwarding engine 202 may be implemented as one or more modules used for both mirroring and forwarding packets from a router to a primary destination (i.e., a destination to which the packet is addressed) and a mirror destination (i.e., the place to which you want the mirror packets to be sent)); and a mirror exit device including a secure mirroring receiver configured to detect and decapsulate the encapsulated encrypted packets from the mirror entry device and to decrypt the encrypted packets (see Regan abstract and paragraph 0022

i.e. a forwarding engine 202 may be implemented as one or more modules used for both mirroring and forwarding packets from a router to a primary destination (i.e., a destination to which the packet is addressed) and a mirror destination (i.e., the place to which you want the mirror packets to be sent)).

Regan does not teach to use an incrementing identifier to indicating an order of the detected packets, to encrypt the detected packets, to encapsulate each of the encrypted packets by adding to the encrypted packet a first header which includes said identifier and an internet Protocol destination address and by also adding a second header which includes a media access control destination address, and an encryption module configured to be utilized by the remote mirroring engine during encryption of the detected packets.

Regan teaches that the mirrored packet are encapsulated and sent via a transport tunnel (see paragraph 0025) but does not go into the way the packets are encapsulated.

Inada teaches to encrypt the detected packets (see column 11 lines 43-52 i.e. encrypts the whole received plaintext pack), to encapsulate each of the encrypted packets by adding to the encrypted packet a first header which includes said identifier and an internet Protocol destination address (see column 11 lines 43-52 i.e. set new IP header) and by also adding a second header which includes a media access control destination address (see column 11 lines 43-52 i.e. then, the ciphertext MAC address resolution block 28 sets the MAC address of the MAC header based on the IP address of the IP header newly set).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used the encapsulation as taught by Inada to encrypt and encapsulate the data packet to further increase the security of the data packet by not allowing other devices to intercept the IP packet and read its data portion (see Inada column 13 lines 39-57). Therefore one would have been motivated to have used the encapsulation as taught by Inada.

Amara teaches incrementing an identifier for indicating a position of the data packet within an order of packets received by an exit device (see Figure 4 element 210 sequence number and column 8 lines 5-24). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a sequence number is used to keep track of each data packet. Therefore one would have been motivated to have a sequence number for each packet.

With respect to claim 18, wherein the encrypting and decrypting is performed under a public-private key encryption scheme (see Amara column 10 lines 6-60).

With respect to claim 19, wherein the encrypting is performed using a public key of a destination device, and wherein the decrypting is performed using a corresponding private key of the destination device (see c Amara column 10 lines 6-60).

With respect to claim 20, a system for secure remote mirroring of network traffic, the system comprising a mirror entry device and a pre-configured destination address associated with a mirror exit device; wherein the pre-configured destination is distinct from original destination indicated in the detected packets, wherein the detected packets are forwarding in unencrypted form towards an original destination address

indicated in the data packet (see Regan abstract and paragraph 0022 i.e. a forwarding engine 202 may be implemented as one or more modules used for both mirroring and forwarding packets from a router to a primary destination (i.e., a destination to which the packet is addressed) and a mirror destination (i.e., the place to which you want the mirror packets to be sent)).

Regan does not teach to use an incrementing identifier to indicating an order of the detected packets, to encrypt the detected packets, to encapsulate each of the encrypted packets by adding to the encrypted packet a first header which includes said identifier and an internet Protocol destination address and by also adding a second header which includes a media access control destination address, and an encryption module configured to be utilized by the remote mirroring engine during encryption of the detected packets.

Regan teaches that the mirrored packet are encapsulated and sent via a transport tunnel (see paragraph 0025) but does not go into the way the packets are encapsulated.

Inada teaches to encrypt the detected packets (see column 11 lines 43-52 i.e. encrypts the whole received plaintext pack), to encapsulate each of the encrypted packets by adding to the encrypted packet a first header which includes said identifier and an internet Protocol destination address (see column 11 lines 43-52 i.e. set new IP header) and by also adding a second header which includes a media access control destination address (see column 11 lines 43-52 i.e. then, the ciphertext MAC address

resolution block 28 sets the MAC address of the MAC header based on the IP address of the IP header newly set).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used the encapsulation as taught by Inada to encrypt and encapsulate the data packet to further increase the security of the data packet by not allowing other devices to intercept the IP packet and read its data portion (see Inada column 13 lines 39-57). Therefore one would have been motivated to have used the encapsulation as taught by Inada.

Amara teaches incrementing an identifier for indicating a position of the data packet within an order of packets received by an exit device (see Figure 4 element 210 sequence number and column 8 lines 5-24). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a sequence number is used to keep track of each data packet. Therefore one would have been motivated to have a sequence number for each packet.

With respect to claim 21, A method for secure remote mirroring of network traffic, the method comprising: remotely configuring an entry device with an destination address (see Regan abstract i.e. data packets, segments, frames, or other forms of encapsulation may be mirrored off of a core network (e.g., IP, TCP); receiving a data packet to be mirrored by the entry device (see Regan abstract i.e. data packets, segments, frames, or other forms of encapsulation may be mirrored off of a core network (e.g., IP, TCP); forwarding the data packet in unencrypted form towards an original destination address indicated in the data packet and forwarding the

encapsulated encrypted packet to the exit device (see Regan abstract and paragraph 0022 i.e. a forwarding engine 202 may be implemented as one or more modules used for both mirroring and forwarding packets from a router to a primary destination (i.e., a destination to which the packet is addressed) and a mirror destination (i.e., the place to which you want the mirror packets to be sent)).

Regan does not teach remotely configuring an exit device at the destination address with a decryption key; incrementing an identifier to indicate a position of the data packets within an order of packets mirrored by the entry device; encrypting a copy of the data packet using the encryption key to form an encrypted packet; generating and adding a header to encapsulate the encrypted data packet, wherein the header includes the mirroring destination address.

Regan teaches that the mirrored packet are encapsulated and sent via a transport tunnel (see paragraph 0025) but does not go into the way the packets are encapsulated.

Inada teaches to encrypt the detected packets (see column 11 lines 43-52 i.e. encrypts the whole received plaintext pack), to encapsulate each of the encrypted packets by adding to the encrypted packet a first header which includes said identifier and an internet Protocol destination address (see column 11 lines 43-52 i.e. set new IP header) and by also adding a second header which includes a media access control destination address (see column 11 lines 43-52 i.e. then, the ciphertext MAC address resolution block 28 sets the MAC address of the MAC header based on the IP address of the IP header newly set).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used the encapsulation as taught by Inada to encrypt and encapsulate the data packet to further increase the security of the data packet by not allowing other devices to intercept the IP packet and read its data portion (see Inada column 13 lines 39-57). Therefore one would have been motivated to have used the encapsulation as taught by Inada.

Amara teaches remotely configuring an exit device at the destination address with a decryption key (see column 8 line 66 – column 9 line 15 i.e. the source device endpoint encrypts the IP packet); incrementing an identifier to indicate a position of the data packets within an order of packets mirrored by the entry device (see Figure 4 element 210 sequence number and column 8 lines 5-24);

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used the encapsulation as taught by Amara to encrypt and encapsulate the data packet to further increase the security of the data packet. Therefore one would have been motivated to have used the encapsulation as taught by Amara.

With respect to claim 22, wherein the remote configuration is performed by way of SNMP (see Amara column 3 line 14 – column 4 line 17 SNMP is included in TCP/IP).

With respect to claim 23, wherein the remote configuration is performed by way of a secure remote protocol (see Amara column 3 line 14 – column 4 line 17).

Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Regan (U.S. 2004/0213232) in view of Inada et al (U.S. Patent # 6,775,769) in view of Amara et al (U.S. Patent # 6,839,338) in further view of Kojima et al (5,280,476).

Regan and Inada do not teach with respect to claim 5, wherein determining the MAC address comprises: determining if a mapping of the IP destination address to the MAC destination address is stored in an address resolution protocol (ARP) cache; if so, then retrieving the MAC destination address from the ARP cache; and if not, then broadcasting an ARP request with the IP destination address and receiving an ARP reply with the MAC destination address.

Kojima teaches wherein determining the MAC address comprises: determining if a mapping of the IP destination address to the MAC destination address is stored in an address resolution protocol (ARP) cache (see Kojima column 5 lines 17-35); if so, then retrieving the MAC destination address from the ARP cache (see Kojima column 5 lines 19-20); and if not, then broadcasting an ARP request with the IP destination address and receiving an ARP reply with the MAC destination address (see Kojima column 5 lines 17-35). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have added a MAC address to the data get to help the data get delivered to its destination across the LAN (see Kojima column 5 lines 17-35). Therefore one would have been motivated to have added a MAC address.

With respect to claim 6, wherein the IP-encapsulated encrypted packet is communicated across multiple intermediate layer 2 domains (see Amara figure 1).

Claim 12, rejected under 35 U.S.C. 103(a) as being unpatentable over Regan (U.S. 2004/0213232) in view of Inada et al (U.S. Patent # 6,775,769) in view of Amara et al (U.S. Patent # 6,839,338) in view of Classon et al (U.S. Patent 6,700,867).

Regan and Amara teach everything with respect to claim 1 above but do not teach truncating the data packet to reduce a size of the data packet prior to encryption. Classon teaches truncating the data packet to reduce a size of the data packet prior to encryption (see column 20 lines 20-53). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have truncated the data packet to satisfy memory (buffer) requirements (see column 20 lines 20-53). Therefore one would have been motivated to have truncated the data packet.

Claim 13, rejected under 35 U.S.C. 103(a) as being unpatentable over Regan (U.S. 2004/0213232) in view of Inada et al (U.S. Patent # 6,775,769) in view of Amara et al (U.S. Patent # 6,839,338) in view of Engwer (U.S. Patent 6,947,483).

Regan Inada and Amara teach everything with respect to claim 1 above but does not teach compressing at least a portion of the data packet to reduce a size of the data packet prior to encryption. Engwer teaches compressing at least a portion of the data packet to reduce a size of the data packet prior to encryption (see column 1 line 52 – column 2 line 6). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have

compressed the data packet. Data transmission between the various access points (APs) and their associated mobile units may involve large amounts of data which may take substantial amount of time and processing power to transmit over the air median. Such data transmissions are costly if the transmitted data is uncompressed (see column 1 line 52 – column 2 line 6). Therefore one would have been motivated to have compressed the data packet.

(10) Response to Argument

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Regan teaches in Abstract and paragraphs 0022-0026, a method for remote mirroring network traffic by receiving a data packet to be remotely mirrored; forwarding the data packet in unencrypted form towards an original destination address indicated in the data packet and forwarding a encapsulated copy of the packet to an exit device associated with the mirroring destination address.

Regan teaches that the mirrored packet are encapsulated and sent via a transport tunnel in paragraph 0025 but does not teach how the packets are encapsulated.

Inada teaches in column 11 lines 43-52 generating and adding a first header and a second header to the encrypted data packet to encapsulate the encrypted data

packet, wherein the first header includes an Internet Protocol destination address corresponding to the destination address (i.e. set new IP header), the second header includes a media access control (MAC) destination address (i.e. then, the ciphertext MAC address resolution block 28 sets the MAC address of the MAC header based on the IP address of the IP header newly set), and the encapsulated encrypted packet comprises an IP-encapsulated encrypted packet including the IP destination address. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have used the encapsulation as taught by Inada to encrypt and encapsulate the data packet to further increase the security of the data packet by not allowing other devices to intercept the IP packet and read its data portion (see Inada column 13 lines 39-57). Therefore one would have been motivated to have used the encapsulation as taught by Inada.

Amara teaches including a sequence number (identifier) in each packet to keep track of the order of each data packet in Figure 4 element 210 sequence number and column 8 lines 5-24. This combination clearly teaches “wherein the first header includes an Internet Protocol destination address corresponding to the destination address and said identifier”. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a sequence number is used to keep track of each data packet. Therefore one would have been motivated to have a sequence number for each packet. Also both Inada and Amara are in the same field of endeavor of secure encapsulation techniques on packet data.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Devin Almeida/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

A Technology Center Director or designee must personally approve the new ground(s) of rejection set forth in section (9) above by signing below:

/Timothy P Callahan/
Director, Technology Center 2400

Conferees:

/Jung Kim/
Primary Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

This examiner's answer contains a new ground of rejection set forth in section **(9)** above. Accordingly, appellant must within **TWO MONTHS** from the date of this answer exercise one of the following two options to avoid *sua sponte* **dismissal of the appeal** as to the claims subject to the new ground of rejection:

(1) **Reopen prosecution.** Request that prosecution be reopened before the primary examiner by filing a reply under 37 CFR 1.111 with or without amendment, affidavit or other evidence. Any amendment, affidavit or other evidence must be relevant to the new grounds of rejection. A request that complies with 37 CFR 41.39(b)(1) will be entered and considered. Any request that prosecution be reopened will be treated as a request to withdraw the appeal.

(2) **Maintain appeal.** Request that the appeal be maintained by filing a reply brief as set forth in 37 CFR 41.41. Such a reply brief must address each new ground of rejection as set forth in 37 CFR 41.37(c)(1)(vii) and should be in compliance with the other requirements of 37 CFR 41.37(c). If a reply brief filed pursuant to 37 CFR 41.39(b)(2) is accompanied by any amendment, affidavit or other evidence, it shall be treated as a request that prosecution be reopened before the primary examiner under 37 CFR 41.39(b)(1).

Extensions of time under 37 CFR 1.136(a) are not applicable to the TWO MONTH time period set forth above. See 37 CFR 1.136(b) for extensions of time to reply for patent applications and 37 CFR 1.550(c) for extensions of time to reply for ex parte reexamination proceedings.